

### Abstract of the Disclosure

A cryptographically secure, computer hardware-implemented modular reduction method systematically  
5 underestimates and randomizes an approximate quotient  
used for computation of a remainder. The randomizing  
error injected into the approximate quotient is limited  
to a few bits, e.g. less than half a word. The computed  
remainder is congruent with but a small random multiple  
10 of the residue, which can be found by a final set of  
subtractions by the modulus. In addition to a  
computational unit and operations sequencer, the  
computing hardware also includes a random or pseudo-  
random number generator for producing the random error.  
15 The modular reduction method thus resists hardware  
cryptoanalysis attacks, such as timing and power analysis  
attacks.